REMARKS/ARGUMENTS

Claim History

The Examiner rejected claims 1-10 and 12-30 under 35 U.S.C. § 103 over Smith in view of Boebert et al.

Status

No claim has been cancelled by the present amendment and claim 31 has been added. Independents claims 1, 12, 17, 28, and 31 with corresponding claims depending therefrom will remain for further consideration.

More Clearly Defined

The claims in this application have been revised to voluntarily further clarify Applicant's unique invention. Applicant maintains that the claims as filed were patentable over the art of record. However, to expedite issuance of this application, reconsideration of the claims in light of the amendments and for the following reasons is respectfully requested.

35 U.S.C. § 103

The Examiner rejected claims 1-10 and 12-30 under 35 U.S.C. § 103 over Smith in view of Boebert et al. This rejection is respectfully traversed.

A central purpose of the present invention is to provide a system which provides end-to-end security of a file so that a user can be assured that the file is the same file that

was sent by the sender and the information has not be altered or read. To this end, several steps are provided by the present invention or prevented by the present invention to ensure the privacy and integrity of the e-mail. Additionally, several steps allow for the process to be carried out by a central escrow computer system connected to a user's computer system so that the user's computer can forward an encrypted document to a server or escrow computer until delivery over a network to a recipient, while the document is secure from prying eyes.

To achieve this purpose, the invention as recited in the claims must ensure that the document is secure from the time that the document leaves the sender until it is received by the recipient. Claim 1 recites several features which define the present invention over the art of record, namely Smith as modified by Boebert. First, the package is encrypted with an "escrow encryption key" prior to storing the package in escrow: "storing the escrow key encrypted package in escrow prior to receiving a public key for the addressee... [and] notifying the addressee of the package stored in escrow." (Claim 1) The Smith patent, when examined carefully, is easily distinguished from the present invention. In the Smith patent, the document never leaves the Sender until the public key is received. "In the event that the certificate authority returns no certificate [col. 5, lines 5-6] ...[u]pon receiving the public key from the Delivery Server [col. 5, lines 31-32] the sender encrypts the secret key with the public key ... [t]he sender then forwards 70 the encrypted document ... to the Delivery Server [col. 5, lines 38-42]. Thus, the document does not leave the Sender until the document has been encrypted with the secret key and the secret ey has been encypted with the intended recipient's public key." Thus the Smith system is little able to achieve the purpose of the present invention of using an escrow system to store a document securely for delivery to a recipient. Smith merely has a Delivery Server which

delivers or "passes through" the package once the public key has been received. The document must be stored at the sender, so the system will not automatically complete the delivery unless the Sender is still connected to the network until the recipient is contacted and decides to respond. This would be highly undesirable, especially if the Sender is connected by telephone line from a distant location running up long distance bills or just having to wait at his location.

Even in an alternative embodiment described in the Smith patent, the sender does send the unencrypted document to the Delivery Server only a non-encrypted document to be encrypted with the public key, but this obviates the entire invention which is to maintain a secure, encrypted document from one end to the other, and is contrary to the claim of storing the escrow key encrypted document.

Claim 31 is a new independent claim which parallels claim 1, but emphasizes that the escrow storage area is remote from the Sender and the Recipient, "transmitting the escrow key encrypted package through the network to an escrow storage area remote from said [Sender's] first computer." Again, the package must be encrypted prior to transmitting and storage, all prior to receiving a public key for the addressee. Only through this process can the system act as an effective escrow agent to store the package delivered in encrypted form until the recipient is ready to receive the package. If the package is unencrypted at any point during transfer or storage at a remote location, then the benefits of the delivery system is lost. Smith does not provide this end to end encryption taught by the present invention.

Boebert does not cure this defect. Boebert et al. is to a non-analogous "Virtual Private Network" and no one looking to cure the defects of a delivery server system would

pick and choose individual elements of transfer protocols from a VPN to fix a mail notification system. Namely, the fact that Boebert has as one of many elements, the ability to decrypt and re-encrypt a document is not enough alone to provide a teaching to Smith. Namely, Boebert does not provide Smith with a separate storage at the Delivery Server to hold a document in escrow while waiting to hear from the Recipient. The document in Smith is held by the sender. "The Delivery Server is responsible for determining the public key of a given recipient and forwarding that key to the Send Client. The Delivery Server is also responsible for delivering the encrypted document and secret key to the intended recipient." (Col. 6, lines 11-14) There is no reason to store the document at the Delivery Server because the public key is already known when the document is sent to the Delivery Server, so the Delivery Server is strictly pass through, unlike the present invention. If anything, the combination would merely affect Smith when the document is unencrypted during delivery over the secure channel to teach encryption of the document using the Public Key, which would already be in possession of the Delivery System before the file leaves the Sender. Additionally, the re-encryption system of Boebert cannot be removed from the entire system of Boebert and placed in another system, especially where no other purpose is provided for the encryption and no teaching of the escrow storage area is provided by either reference. Smith is already aware of "encryption" and "data storage" and would thus be taught little from Boebert on how to secure documents. However, since there is no storing of the document on the Delivery Server, there is no retrieval from storage of an encrypted document for re-encryption as allegedly taught by Boebert. And further, Boebert is completely not analogous being to a VPN and requires a Public Network to utilize the pieces of the system allegedly taught by Boebert. Additionally, Boebert appears to deal with a user accessing a secure computer ("pulling data"), rather than an

escrow agent sending data out to a user ("pushing data") and thus has no analogous application in Smith.

Additionally Smith states plainly that if the document is to be encrypted with the public key then it will be unencrypted up to that point to "minimize processing time when a public key cannot be retrieved." (Col. 5, lines 32-37) Boebert teaches away from Smith to encrypt and then decrypt and re-encrypt a document as allegedly taught by Boebert, and Boebert provides no advantage for doing so.

For at least these reasons, claims 1 and 31, and their corresponding dependent claims should be allowed over the art of record.

Claim 12 further requires that the stored escrow-encrypted package is unencrypted and re-encrypted with the public key prior to transmission on the network. Claim 12 as amended now clarifies that the package must be encrypted prior to storage in escrow and prior to notification of the addressee of the stored package. No such storage is provided by Smith, which waits until receiving the public key before releasing the file from the Sender. As discussed above, although Boebert is alleged to show that a virtual private network ("VPN") has encryption and re-encryption, it does not add the missing feature of storing a file in escrow. Further, the package is transmitted out to the addressee, and thus Boebert is non-analogous art and would have no reason to re-encrypt the file since it was never stored on an escrow system of Smith. There must be some reason to combine Smith and Boebert other than the hindsight provided by the current invention. Further, as discussed above, to re-encrypt would teach away from the Smith patent which provides for minimizing processing time by leaving the file unencrypted prior to encryption with the public key at the time the package is sent to the Recipient. For at least these reasons,

Smith and Boebert would not combine to form the presently claimed invention, even if there were a reason to combine the references. Claim 12 and its dependent claims should therefore be allowed over the art of record.

Claim 17 recites an "escrow manager" which is not provided in the prior art. Although the Examiner has argued that the "secret key" parallels the "escrow key," this does not provide for the absence of the escrow manager that holds the package in escrow. In fact, according to Smith (and unmodified by Boebert), the package is not sent by the Sender until the public key is received, at which time it is sent to the Delivery Server for immediate delivery as there is no reason and no teaching for holding the package further. There is no teaching in Smith or Boebert of holding the package once it is encrypted in any kind of storage, only an unencrypted package which would be unsecure. In any case, the unencrypted package is delivered immediately by the Delivery Server after encryption with the public key, which has already been received. There is no teaching or comparable automated escrow agent in the Smith patent which holds the encrypted package while waiting to hear back from the recipient or prior to receiving the public key. Boebert, drawn to an non-analogous virtual public network, cannot fix this and certainly provides no teaching except that of encryption, which is already well known to Smith. Boebert does not disclose transmitting a file to a holding agent ("escrow agent") for holding the file while authentication occurs. Neither can the elements of Boebert be picked from and chosen at random to apply to Smith without further reason. Further Boebert is drawn to "manual" access of a file stored by one user and accessed by another user. It has no analogous use on an automated system lacking an escrow agent. Since there is no escrow storage area, there is no teaching of a need to provide an escrow storage area or improving the security system of the Smith patent using such a system.

Only by the teaching of the present invention and recognition of the need for end to end security and the use of an automated escrow agent having a computer readable medium to hold the file released by the sender would there be a need for holding the package in its encrypted form to provide security and accountability to the package. For at least these reasons, claim 17 and its dependent claims should be allowed over the art of record.

Claim 28 also requires that a package be encrypted prior to transmission over the network or storage in escrow. The package can be encrypted with an escrow encryption key and transmitted to an escrow storage area, or the package can be encrypted by a public key and transmitted over the network to a recipient. However, the claim specifically recites that the package cannot be transmitted over the network without being encrypted. Smith not only allows the package to be transmitted without being encrypted (see col. 5, lines 60-67), but teaches that this is preferable. The document is unencrypted to save processing speed since the file will be eventually encrypted with the public key or not sent at all. (Col. 5, lines 32-37). However, this transfer leaves the package vulnerable to viewing and/or modification. The purpose of the present invention is to provide an end to end secure package transmission system. Boebert provides a VPN system, but is merely for storing a file on a Server by one user and subsequent access by a second user, and is not analogous for an automated system having an internal storage (such as the present invention) or no storage (the Smith patent). There would be no reason to provide an extra escrow storage area on the Smith patent because the package is not sent from the Sender until the recipient's public key is known. At that time, the package is merely passed through the delivery server to the recipient. No escrow manager or escrow storage is provided, listed or taught by Smith. The mere fact that Boebert has a harddrive or other

storage would not teach any reason for the Smith patent to incorporate an escrow storage area for the file without the hindsight of the current invention. For at least these reasons, claim 28 should be allowed.

Summary

Applicants have made a diligent and bona fide effort to answer each and every ground for rejection or objection to the specification including the claims and to place the application in condition for final disposition. Reconsideration and further examination is respectfully requested, and for the foregoing reasons, Applicant respectfully submits that this application is in condition to be passed to issue and such action is earnestly solicited. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Robert N. Blackmon, Applicants' Attorney at 703-684-5633 to satisfactorily conclude the prosecution of this application.

Dated: December 22, 2004

Respectfully submitted,

Merek, Blackmon & Voorhees, LLC
673 S. Washington St.
Alexandria, Virginia 22314
Tel. 703-684-5633
Fax. 703-684-5637
E-mail: RNB@ BlackmonLaw.com

Robert N. Blackmon
Reg. No. 39494
Attorney/Agent for Applicant(s)